COMPUTER NETWORK SECURITY SYSTEM

Field of the Invention

The present application relates generally to providing secure communications over a computer network such as the Internet.

Background of the Invention

The Secure Socket Layer (SSL) is a well known security protocol developed by Netscape ® for transmitting private documents securely over the Internet. The SSL protocol works by using a private key to encrypt data that's transferred over an SSL connection. Many web sites use the SSL protocol to obtain confidential user information, such as a credit card number. The use of this protocol may not be desirable for all uses, however, because the use of SSL can require the purchase of a certificate.

A device that can authenticate users over the Internet is the Web/SNMP management card that has part number AP9606 and is manufactured by the American Power Conversion, Corp. of West Kingston, RI. When the AP9606 card is first installed, the user programs it with an authentication phrase. This authentication phrase becomes a shared secret between the AP9606 card and the user. The AP9696 card provides security by transmitting an applet from the AP9606 card to a web browser, and the applet uses the shared secret to authenticate the user. Additionally, the AP9606 card also secures form data using this applet by hashing form fields with the shared secret. The AP9606 card can also provide management of uninterruptible power supplies (UPS's) via multiple open standards like Telnet, HTTP, and SNMP. Through the

In another embodiment of the invention, a system is provided for authenticating a user of a computer over a computer network. The system includes a web server coupled to the computer network, wherein the web server is programmed to: transmit an applet having a challenge string and a first encryption key; receive a login packet having the challenge string and a password that is encrypted using the first encryption key; decrypt the password; and authenticate the password by using information provided by an authentication provider.

In yet another embodiment of the invention, an article of manufacture is provided that includes a computer readable medium having computer readable program code for authenticating a user of a client computer over a computer network, the computer readable program code including instructions for: causing the computer system to transmit an applet having a challenge string and a first encryption key; causing the computer system to receive a login packet having the challenge string and a password that is encrypted using the first encryption key; causing the computer system to decrypt the password; and causing the computer system to authenticate the password by using information provided by an authentication provider.

The web server can be a computer program installed on the computer or a server computer. The authentication provider can be an authentication server or can be a software program installed on the computer in communication with the computer network.

An advantage of embodiments of the present invention is that a computer can provide secure Internet communications using a web browser that does not support SSL. Yet another advantage of embodiments of the present invention is that a computer can each coupled to a computer network 13, such as a wide area network (WAN), a local area network (LAN) or the Internet. A web server 14 and an authentication server 16 are also coupled to the computer network 13. The authentication server 16 assists the web server 14 in providing secure access to a web page on the web server 14. An uninterruptible power supply (UPS) 15 can be coupled to the web server to provide power to the computer in case of a power failure to the computer.

One of the computers 12a-c can access the web servers 14 through network 13 to obtain a web page having information, for example, about the status of UPS 15. A user on one of the computers 12a-c can also access a web page on the web server 14 to obtain information about the UPS 15 and may be able to configure or control the UPS 15.

FIG. 2 shows an illustrative example of how a user can be authenticated to access information from the web server 14 using the system 10 of FIG. 1. Initially, a user is provided with a password known to or recognizable by the authentication server 16. This can be accomplished in several ways, such as providing the user with the password electronically through e-mail or a web page, or providing the user with the password through the mail, over the telephone or in person.

After a user has received a valid password known by the authentication server 16, the user can attempt to access a secured web page on web server 14. When the user of the computer 12 first accesses the secured web page on web server 14, the user's web browser is redirected to a URL of a login page. The web server 14 transmits two frames for the login page, one of the frames being visible to the user and the other being hidden from view of the user. The visible frame contains a form having fields for the user to enter a username, a password or other credentials. The second hidden frame has no provider 16. The authentication provider 16 can be located on a separate server as shown in FIG. 6 or can be a separate process running somewhere in the user's network that integrates with the user's general security system, such as the Domain Controller from Windows NT 4 ® or Keberos, which is an open authentication scheme developed at the Massachusetts Institute of Technology.

The web server requests an encryption key from the authentication provider 16 and encrypts the user's password and/or credentials using the encryption key transmitted from the authentication provider 16. The web server 14 then transmits to the authentication provider 16 authentication data including the username and encrypted credentials and requests that the authentication provider verify the authentication data. The authentication provider 16 receives and decrypts the authentication data and validates it using a security method, such as Windows NT ® system call.

The authentication provider 16 then creates a response for the web server 14 by hashing the decrypted credentials and a secret string. As noted above, a hash algorithm such as, for example, the MD5 hashing algorithm can be used. The secret string is preferably known only to the integration provider and the web server and can be a text message, such as "PASSWORD OK." The hash code 26 is transmitted to the web server 14 and the web server verifies that it is correct. If the hash code 26 is correct, then the web server 14 grants the user access to the web site.

Once the web server 14 has granted the user access to the web site, the web server enables the session ID provided to the user with the security applet 18 such that it can now be used to view and retrieve web pages. The preferable way to use the user's session ID is to have the session ID as part of the URL of each page request to the web

A method 40 for authenticating a user of a computer over the computer network of FIG. 1 will now be described with reference to FIG. 4. At 42, an applet having a unique session identification and a first encryption key is transmitted to a computer. The applet can be transmitted by a web server that can be a server coupled to the network or a computer program installed and running on the computer. At 44, a login packet is received from the computer that has the session identification, a user name, a password and a first hash of the session identification, the user name, and the password. In the login packet, the session identification, the user name, and the password are encrypted using the first encryption key. At 46, the session identification, the user's name, and the password contained in the packet are decrypted. At 48, a second encryption key is received from an authentication provider. The authentication provider can be a server having a security program running thereon or it can be a program accessible by the network. At 50, the user name and the password are encrypted using the second encryption key and transmitted to the authentication provider. At 52, a second hash of the password and a character string is received from the authentication provider. At 54, it is determined from the character string if the password is correct.

A method 60 for authenticating a form submitted by the user of a computer over the computer network of FIG 1 will now be described with reference to FIG. 5. The method of FIG. 5 can be used in conjunction with the method of FIG. 4. At 62, a security applet, a form and a second unique sequence ID are submitted to the computer. The form and the second unique sequence ID can be transmitted by a web server that can be a server coupled to the network or a computer program installed and running on the computer. At 64, response data to the form and a hash of the second unique sequence